Exhibit B

ZHIYUAN SUN

JAN 26, 2023

Aave purchases 2.7M CRV to clear bad debt following failed Eisenberg attack

Following a failed short attack, DeFi exploiter Avraham Eisenberg was liquidated from Aave at a loss of $10 million.

3313 19 1:54

Collect this article as an NFT >

According to a new post on Jan. 26, Marc Zeller, integrations lead at decentralized finance (DeFi) lending protocol Aave, stated that the firm purchased 2.7 million Curve (CRV) tokens, which would clear "excessive remaining bad debt" within the next 15 hours over a dozen transactions. The move follows the community approval of Aave Improvement Protocol (AIP) 144, which deployed a swap contract that acquires 2.7 million units of CRV, with a USD Coin USDC ▼ $1.00

spend limit of $3,105,000 and a maximum unit value of $1.15 per CRV.

The bad debt on the Aave protocol resulted from a sophisticated exploit that took place on Nov. 23. Avaraham Eisenberg, who previously drained DeFi protocol Mango Markets and caused $47 million in net damages, took on a series of heavy volume short CRV positions on Aave in an attempt to orchestrate a short squeeze and force developers to buyback his positions at upward of 100% slippage due to lack of liquidity.

However, it turned out Aave had much more liquidity than anticipated, and Eisenberg reportedly lost $10 million on the trade. Nevertheless, some slippage occurred as a result of the incident, and Aave was left with a total of 2.656 million CRV in bad debt while liquidating Eisenberg's positions.

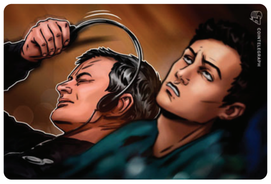
The same day, Mango Markets filed a lawsuit against Eisenberg, asking the court to rescind its $47-million bounty agreement with the hacker for his role in the $117-million exploit on Oct. 12, 2022. The United States Securities and Exchange Commission has charged Eisenberg with stealing $117 million in digital assets. Eisenberg was arrested in Puerto Rico by the Federal Bureau of Investigation on Dec. 27, 2022, on charges of commodities manipulation and commodities fraud.

Avraham Eisenberg (right) during an interview. Source: YouTube, "Unchained" podcast

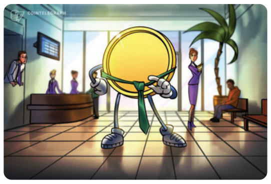
#Blockchain #Cryptocurrencies #DeFi #Aave

RELATED NEWS

What is Solana (SOL) Pay, and how does it work?

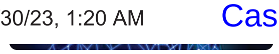


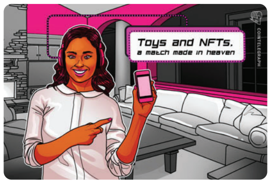
Opinion: 3 tips for trading Ethereum this year



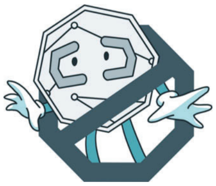
How crypto tokens (but not Bitcoin) will outperform stocks in 2023 — Arca’s CIO explains

DeFi, DAOs and NFTs: Crypto is redefining how charities raise funds





NFT Steez and Cryptoys CEO discuss the future of toys and entertainment within Web3



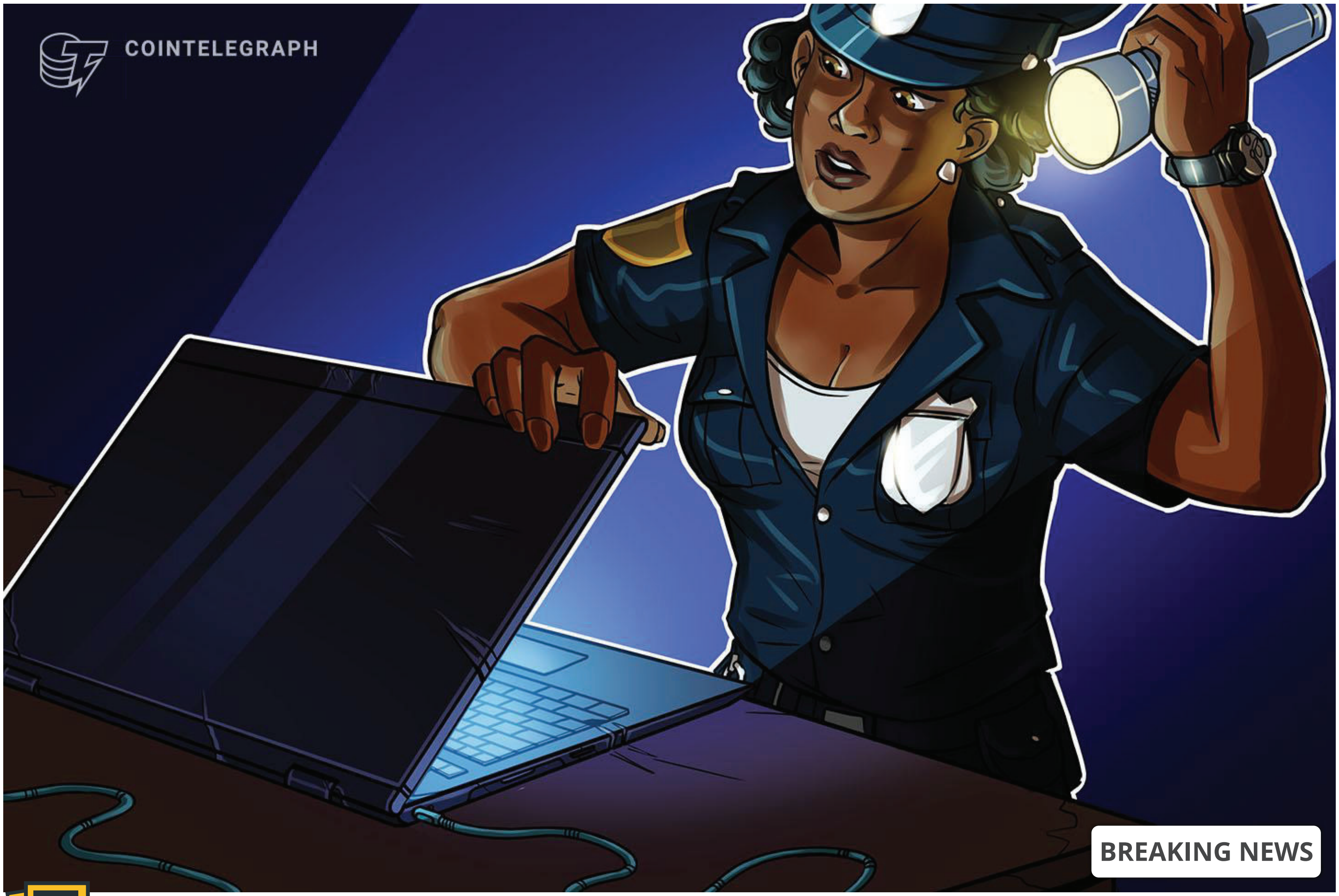
ZHIYUAN SUN

JAN 26, 2023

US Justice Department seizes website of prolific ransomware gang Hive

The group is known to have targeted critical infrastructure, healthcare providers and more over the past two years.

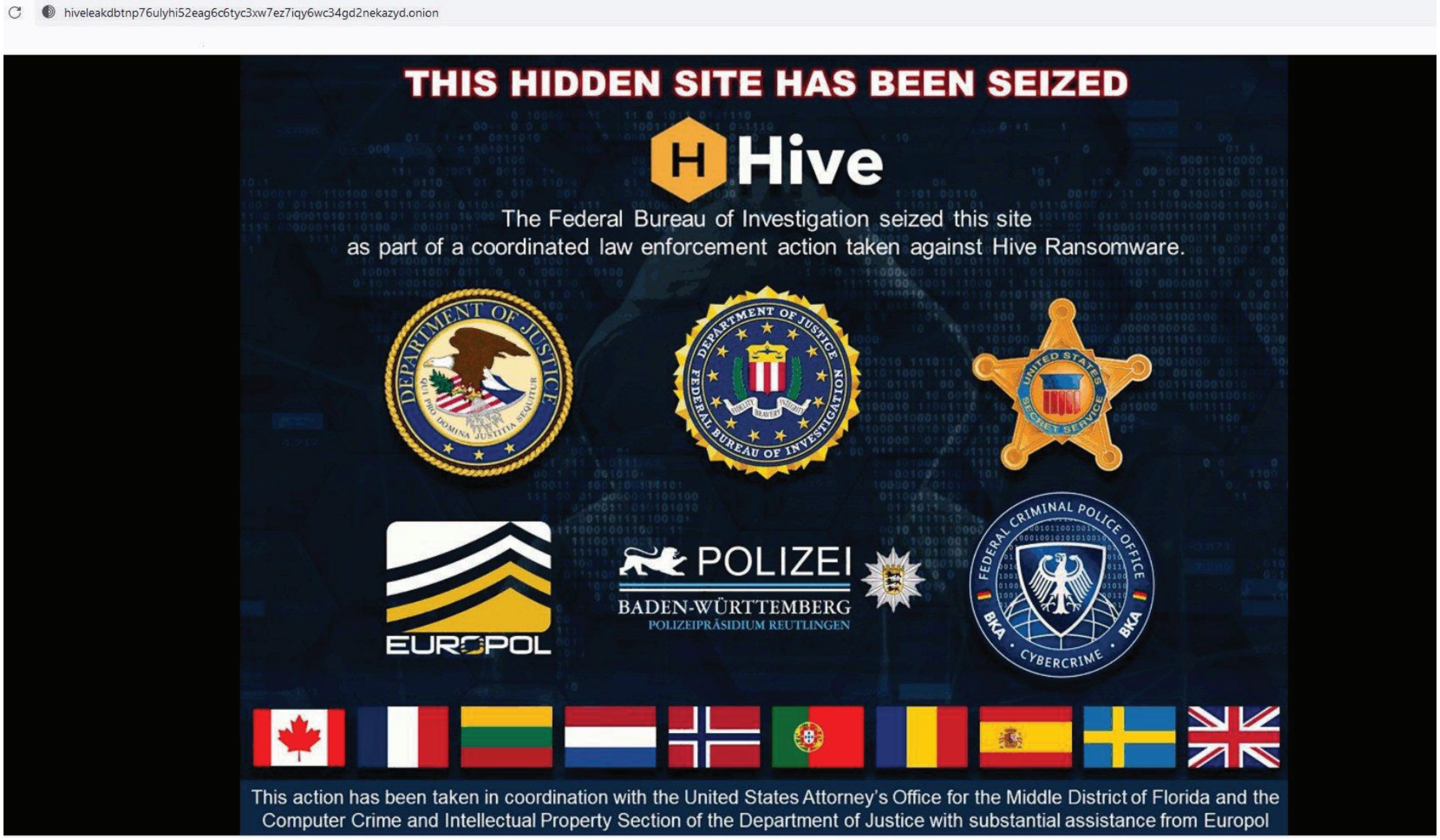
3980 36 0:49



Collect this article as an NFT >

According to United States Federal Bureau of Investigation Director Christopher Wray on Jan. 26, international law enforcement groups have dismantled the infamous Hive cryptocurrency ransomware gang. He claimed that the operation has recovered over 1,300 decryption keys for victims since July 2022 and prevented $130 million in ransomware payments. Officials raised the example of one incident where a Hive ransomware attack on a Louisiana hospital was thwarted by law enforcement, saving the victim from a $3-million ransom payment.

Ghost servers were reportedly seized Wednesday night in an international law enforcement effort between U.S. authorities, the German Reutlingen Police Headquarters, the German Federal Criminal Police, the Netherlands National High Tech Crime Unit and Europol to track ransom payments, seize them back to victims, and dismantle the network's infrastructure.



hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion

THIS HIDDEN SITE HAS BEEN SEIZED

Hive

The Federal Bureau of Investigation seized this site
as part of a coordinated law enforcement action taken against Hive Ransomware.

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
EUROPOL
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM REUTLINGEN
FEDERAL CRIMINAL POLICE OFFICE
BKA
CYBERCRIME

This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

Hive network dark web address has been taken down by law enforcement. Source: Twitter

The organization had been infiltrated by undercover agents since July 2022. As told by Wray, law enforcement gained "clandestine, persistent" access to Hive's control panels since that time and had been secretly helping victims recover their assets and locked devices unbeknownst to Hive.

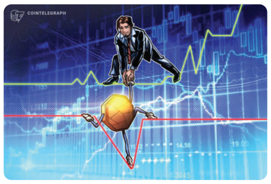
Hive was behind a series of notorious ransomware incidents, such as the April-to-May 2022 Costa Rica public health service and social security fund cyberattack. The group locked key digital infrastructure and demanded $5 million in Bitcoin BTC ▲ $23,724 ransom payments for the restoration of services. Over 4,800 individuals reportedly missed their medical appointments in

the first few days following the attack. Despite the successful enforcement action, Wray also warned:

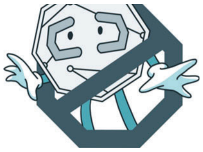
> “Unfortunately, during these past seven months, we found that only about 20% of Hive’s victims reported potential issues to law enforcement. Here, fortunately, we were still able to identify and help many victims who didn’t report in. But that is not always the case. When victims report attacks to us, we can help them — and others, too.”

#Blockchain #Ransomware #United States

RELATED NEWS



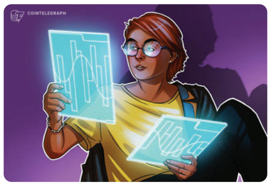
What is impermanent loss and how to avoid it?



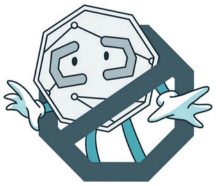
The state of Solana: Will the layer-1 protocol rise again in 2023?

90% of businesses adopting blockchain technology, data

One of the largest US colleges has begun teaching students about Bitcoin



Bitcoin inches closer to a 10-year record, as other stats turn bullish



Are you a journalist
or an editor?

Join us

COINTELEGRAPH NEWSLETTER

Email

Subscribe

Terms of services and Privacy policy